

**KIRBY McINERNEY LLP**

Robert J. Gralewski, Jr. (CSB# 196410)

Fatima G. Brizuela

600 B Street, Suite 1900

San Diego, CA 92101

Telephone: (619) 398-4340

bgralewski@kmlp.com

fbrizuela@kmlp.com

*Attorneys for Plaintiff*

[Additional counsel listed on signature page.]

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN JOSE DIVISION**

ARTESIA GENERAL HOSPITAL, a  
New Mexico not-for-profit corporation,  
individually and on behalf of all others  
similarly situated,

Plaintiff,

v.

INTEL CORPORATION,

Defendant.

Case No.:

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

Judge:

## **INTRODUCTION**

1  
2           1.       General Hospital (“AGH” or “Plaintiff”), a not-for-profit health care provider in  
3       Artesia, New Mexico, brings this class action complaint against Intel Corporation (“Intel” or  
4       “Defendant”), to recover substantial damages resulting from profound, fundamental, and incurable  
5       security defects in central processing units (“CPUs”) designed, manufactured and marketed by Intel  
6       that render patients’ medical records and other protected information vulnerable to hacking.

7           2.       Intel CPUs provide the “brains” of the majority of servers and personal computers  
8       (“PCs”), along with those of other devices, utilized in the health care and other industries. In  
9       January 2018, Intel disclosed that virtually every CPU it had manufactured and sold during the past  
10      decade or more suffered from a number of security vulnerabilities, known as “Meltdown” and  
11      “Spectre.” While distinct, these vulnerabilities have put at risk sensitive data such as user names,  
12      passwords and encryption keys. The flaws in Defendant’s CPUs were the result of Intel’s decision  
13      to prioritize performance over security.

14          3.       Health care providers such as AGH are obligated by federal law under the Health  
15      Insurance Portability and Accountability Act (“HIPAA”) and the American Recovery and  
16      Reinvestment Act (“ARRA”) to protect their patients’ medical records and to make those records  
17      available to them in a secure manner via Internet-connected servers. AGH relied upon Intel’s  
18      representations that its CPUs were secure and fit for use in servers, PCs and other devices that  
19      stored or accessed sensitive patient medical records.

20          4.       As a result of the defects disclosed by Intel, and in order to comply with its privacy  
21      obligations, AGH has been and will be required to (a) undertake temporary measures to mitigate  
22      the security risks posed by “Meltdown” and “Spectre,” which have the side effect of slowing the  
23      performance of its computing resources; (b) incur additional costs monitoring its computing  
24      resources for security breaches; and (c) replace its computing resources on an accelerated schedule  
25      and at significant expense with CPUs that, when available, are not susceptible to these  
26      vulnerabilities.

27          5.       The enormous costs in responding to the “Meltdown” and “Spectre” vulnerabilities  
28      are being borne by thousands of entities throughout the country that, like AGH, are entrusted with

sensitive third-party data. Plaintiff brings this action individually and on behalf of a Class of all similarly situated entities in the United States that are subject to HIPAA or other federal laws or regulations imposing standards of care with respect to the protection of third-party information and that purchased servers, PCs or other devices with the defective Intel CPUs.

## **PARTIES**

### **A. Plaintiff**

6. Plaintiff AGH is a non-profit health care provider organized under the laws of the State of New Mexico which primarily does business in Artesia, New Mexico. Plaintiff's mission is to be a provider of high quality patient-focused health care that is readily accessible, cost effective and meets the needs of the citizens of the Southeastern New Mexico communities it serves. To that end, Plaintiff spends more than \$3 million annually on information technology ("IT") capital and operations. AGH was named by *Hospitals & Health Networks* among "Health Care's Most Wired" in 2017.

7. Plaintiff has purchased servers, PCs and other devices with Intel CPUs that include the vulnerabilities described throughout this Complaint.

### **B. Defendant**

8. Defendant Intel is a Delaware corporation with its principal place of business in Santa Clara, California. Intel designs, manufactures and markets computer products, including CPUs, worldwide.

## **JURISDICTION AND VENUE**

9. This Court has subject matter jurisdiction over this controversy pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because (a) the proposed Class, defined below, consists of more than one hundred members; (b) the parties are minimally diverse, as members of the proposed Class are citizens of states different than Intel's home state; and (c) the aggregate amount in controversy far exceeds \$5 million, exclusive of interests and costs.

10. This Court has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367.

11. This Court has personal jurisdiction over both parties. AGH submits to the Court's jurisdiction. Intel's headquarters and principal place of business are located within this District.

12. Venue is proper in this District under 28 U.S.C. § 1391 because Intel maintains its principal place of business within the District and a substantial part of the events giving rise to Plaintiff's claims occurred here.

### **INTRADISTRICT ASSIGNMENT**

13. Assignment to the San Jose Division of this District is proper under Local Rule 3-2(c)-(e) because a substantial part of the acts or omissions underlying Plaintiff's claims occurred in Santa Clara County.

### **FACTUAL BACKGROUND**

#### **I. Federal Law Obligates Health Care Providers to Create, Maintain and Protect Patient Medical Records.**

14. Health care providers such as AGH are subject to obligations under the ARRA, HIPAA, and attendant regulations and other bodies of law, which impose national standards with respect to the secure storage and handling of confidential patient information.

15. The ARRA requires health care providers like Plaintiff to make "meaningful use" of electronic health records ("EHR") to engage patients and family and to maintain privacy and security of patient health information.

16. HIPAA establishes national standards that require health care providers and their business associates, to develop and follow procedures that ensure the confidentiality and security of protected health information ("PHI"), including electronic PHI ("ePHI"), when it is transferred, received, handled, or shared.

17. Plaintiff and other health care providers are subject to fines imposed by the Office of Civil Rights ("OCR") of the United States Department of Health and Human Services ("HHS") for violations of HIPAA. OCR may impose annual fines up to \$1.5 million on a health care provider for violations of the same HIPAA provision.

1 **II. Intel CPUs Utilized by Health Care Providers and Other Class Members Contain**  
2 **Significant Security Flaws that Place Protected Data at Risk.**

3 18. Health care providers like Plaintiff and other firms subject to heightened privacy  
4 standards under federal law routinely utilize Intel CPUs in their servers, PCs and other computing  
5 devices to generate, analyze and store ePHI, EHR and similar protected information.

6 19. Intel dominates the markets for CPUs used in servers and PCs, with shares estimated  
7 to be in excess of 90% and 80%, respectively, in 2017. Intel markets its widely-used CPUs as being  
8 fit to “prevent exposure to malicious code, viruses, cyber espionage, malware, and data theft.”  
9

10 20. Intel clearly understands the importance of security to health care providers and  
11 others subject to HIPAA. Intel’s web site, for instance, states: “Protection of personal health  
12 information is a critical priority. Intel®-based technologies can support the need for compliance  
13 with local regulation of health care information such as the HIPAA privacy and security rule.”  
14 That same web page warned that “[t]he financial impact from security breaches in the United States  
15 averaged more than USD 5.2 million per event in 2011.”

16 21. In June 2017, a team of researchers at Google’s Project Zero reportedly alerted Intel  
17 of a number of security flaws in Intel CPUs that have existed in virtually every CPU manufactured  
18 and sold by Defendant during at least the past decade. Google’s researchers publicly announced  
19 these security flaws in January 2018.

20 22. Security researchers have publicly detailed three vulnerabilities: one called  
21 “Meltdown” and two referred to as “Spectre.” These vulnerabilities are “privilege escalation” flaws,  
22 meaning that computer code running in less secure user programs (e.g., web browsers, email clients,  
23 and media applications) can surreptitiously access secure kernel or other computer memory to gain  
24 access to sensitive data such as user names, passwords, and encryption keys.  
25

26 //

27 //

28 //

23. An article in *The New York Times* titled “Researchers Discover Two Major Flaws in the World’s Computers,” described the vulnerabilities as follows:

Computer security experts have discovered two major security flaws in the microprocessors inside nearly all of the world’s computers.

The two problems, called Meltdown and Spectre, could allow hackers to steal the entire memory contents of computers, including mobile devices, personal computers and servers running in so-called cloud computer networks.

24. The vulnerabilities are the result of Intel’s decision to achieve performance at the cost of security. Upon information and belief, Intel was or should have been aware of the security flaws prior to Google’s disclosure.

25. “Proof of concept” sample code, which demonstrates how these vulnerabilities could be exploited, has been made available in a variety of programming languages including C++, JavaScript, and C.

**B. Intel’s Modern Central Processing Units**

26. User programs are often made up of CPU instructions that are ordered to be processed and executed serially, one after the other, akin to water moving through a single pipeline. Intel’s CPUs contain more than one “pipeline” for ordering and executing a user program’s instructions. A single-pipeline CPU would take eight cycles to process eight instructions; a CPU with eight pipelines could, under ideal circumstances, process those same eight instructions in one cycle.

27. In order to take advantage of multiple pipelines, Intel’s CPUs make “guesses” as to what CPU instructions may be executed after any particular instruction via a process known as “branch prediction.” Branch prediction utilizes algorithms to determine what instructions are most likely to be executed after another instruction (the “prime instruction”) gathers the predicted instructions and data inputs from memory and speculatively executes those instructions in anticipation of providing the results after execution of the prime instruction.

//

//

1           28. While Intel's implementation of branch prediction and speculative execution in its  
2 CPUs has greatly increased the performance of those processors, its particular design decisions  
3 have introduced grave security flaws.

4           **C. Intel's "Spectre" Design Flaws**

5           29. The "Spectre" security flaws are integral to the design of Intel CPUs and utilize  
6 speculative execution of privileged code. Computer programs generally consist of a series of  
7 repetitive and in-order operations. Intel CPUs take advantage of the repetitive nature of computer  
8 programs by analyzing patterns of past operations to predict future operations. The CPUs then  
9 speculatively gather data from system memory to execute those future operation to quickly provide  
10 the result to the underlying program. A malicious program can train the CPU to predict that  
11 otherwise protected memory will be relevant to a future operation and make that protected memory  
12 available to the malicious program.

13           30. In the context of PCs, malicious programs such as pretextual advertisements in web  
14 browsers can be used to obtain usernames and passwords that provide access to sensitive, valuable,  
15 and confidential data, including patient records, financial information, and client files. In addition  
16 to being attacked via web advertising, computers are susceptible to these attacks via email, instant  
17 messaging, and traditional malware.

18           31. The "Spectre" threat to cloud-based servers is particularly extreme. Cloud-based  
19 virtual server hosting is increasingly common with vendors such as Microsoft, Amazon, IBM,  
20 Salesforce.com, SAP, Oracle, Google, ServiceNow, Workday, VMware, and others providing  
21 shared server resources directly and indirectly to consumers like Plaintiff AGH. In this  
22 circumstance, vendors utilize a single Intel CPU to provide multiple virtual CPUs and servers to  
23 customers.

24           32. A malicious actor could exploit Intel's "Spectre" design flaws by, for example,  
25 purchasing a virtual server in the cloud and running a program that permits access to other virtual  
26 servers running on the same Intel CPU. Such a malicious server sharing space with servers for  
27 hospitals, banks, and law firms could gain complete access to the memory of those virtual servers  
28 and, consequently, gain complete access to all of servers' sensitive data.

1           **D. Intel's "Meltdown" Design Flaw**

2           33. "Meltdown" is a hardware vulnerability that tricks the CPU into speculatively  
3 loading data that has been marked unreadable or "privileged." This flaw potentially allows  
4 malicious programs to request protected kernel memory and to access copies of the protected  
5 memory.

6           34. Modern processors perform speculation around memory accesses; Intel's CPUs,  
7 however, do so in a particularly aggressive way. Metadata associated with operating system  
8 memory determines whether it can be accessed by user programs or is restricted to the kernel. Intel  
9 CPUs allow programs to speculatively use kernel data, with the access check (which verifies  
10 whether the kernel memory is accessible to a user program) occurring only sometime after the  
11 instruction starts executing. While speculative execution is blocked when the check occurs, the  
12 impact that speculation has on the CPUs cache can be used to infer the values stored in kernel  
13 memory.

14           35. As a result of the "Meltdown" vulnerability, Intel's CPUs are potentially susceptible  
15 to JavaScript exploits that allow attackers to obtain sensitive web browser information, including  
16 cookies, credentials, passwords, or payment information a user has entered into a browser. In the  
17 case of Plaintiff and other Class members, that browser data could also include PHI or other  
18 protected third-party information.

19           **E. Intel's "Meltdown" and "Spectre" Design Flaws Cannot be Completely Fixed in**  
20 **Existing CPUs.**

21           36. While the security risks associated with "Meltdown" and "Spectre" can be  
22 mitigated, they cannot be fixed in all instances.

23           37. Software patches have been issued for various operating systems (including  
24 Microsoft's Windows, Apple's macOS, and Linux) to mitigate against "Meltdown" and "Spectre."

25           38. In some instances, software running on Intel CPUs and microcode running within  
26 Intel CPUs can be modified to reduce, but not eliminate, the risk. However, when available, these  
27 techniques reduce the performance of the CPUs, particularly for CPU operations involving  
28 numerous input/output operations.



39. In other instances, no mitigation technique is available, and the Intel CPU is inherently insecure.

**III. Intel's CPU Security Flaws Have Damaged and Will Damage Health Care Providers and Other Entities Subject to Heightened Privacy Standards.**

40. Shortly after the "Meltdown" and "Spectre" flaws were disclosed publicly, OCR reportedly sent an email update that urged HIPAA-covered entities to mitigate the vulnerabilities as part of their risk management processes. Given the nature of the CPU flaws, failure to mitigate places at risk the confidentiality, integrity, and availability of protected health information.

41. On January 12, 2018, HHS's Health Care Cybersecurity and Communications Integration Center ("HCCIC") issued a technical report on the "Meltdown" and "Spectre" vulnerabilities, which noted "[m]ajor concerns" for the health care sector. These included, but were not limited to:

- Challenges identifying vulnerable medical devices and accessory medical equipment and ensuring patches are validated to prevent impacts to the intended use.
- Cloud Computing: Potential PHI or Personally Identifiable Information (PII) data leakage in shared computing environments
- Web browsers: Possible PHI/PII data leakage
- Patches: Potential for service degradation and/or interruption from patches[.]

42. Plaintiff and other Class members have incurred and will continue to incur costs to monitor protected information, including patient ePHI and EHR, for data breaches and other malicious activity. These monitoring costs are above and beyond the costs that would be incurred as part of their ordinary risk management processes. Because the Intel CPU flaws can be mitigated, but not completely fixed, on existing hardware, these additional monitoring costs will continue until such time as Plaintiff and Class members purchase new CPUs that are not subject to the security risks described above.

//

//

43. Additionally, Plaintiff and Class members have been required to expend resources to monitor and maintain their computing resources in connection with Intel's security flaws. By way of example, various of Intel's "patches" supposedly designed to mitigate Intel's security defects are themselves defective and cause substantial reliability issues in affected PCs and servers.

44. As the risks posed by "Meltdown" and "Spectre" to protected information become better understood, Plaintiff and other Class members will be required to engage in additional, costly mitigation techniques, including devoting increased labor to the heightened monitoring of their Intel-based systems for security breaches, the procurement and installation of software designed to avoid Intel's CPU defects, and procurement of additional computer hardware to compensate for the reduced performance of mitigated but still dangerously insecure Intel CPUs.

45. Intel has announced that future generations of its CPUs will not contain these defects. If and when Intel corrects its design defects and begins marketing CPUs without the flaws described above, Plaintiff and other Class members will be compelled to accelerate their purchases of this new equipment, prematurely and outside normal replacement cycles, to eliminate the security risk created by Intel's design decisions. Consequently, Plaintiff and other Class members will sustain additional damages by expending the costs necessary to upgrade to non-defective computers and servers.

### **CLASS ACTION ALLEGATIONS**

46. Plaintiff brings this action on behalf of itself and as a class action under Rule 23(a) and (b)(3) of the Federal Rules of Civil Procedure seeking damages on behalf of itself and Class Members nationwide (the "Class"):

All persons or entities in the United States that are subject to federal regulations imposing standards of care with respect to the protection of confidential third-party information and that purchased (a) one or more Intel CPU, or (b) one or more servers, PCs or other device containing Intel CPUs.

47. Excluded from the Class are Intel, including any of its subsidiaries or affiliates; any entity in which Intel has a controlling interest; and any person who is an officer or director of the aforementioned entities.

1           48. While Plaintiff does not know the exact number of the members of the Class,  
2 Plaintiff believes there are thousands of entities.

3           49. Common questions of law and fact exist as to all members of the Class. Such  
4 questions of law and fact common to the Class include, but are not limited to:

- 5           a. Whether Intel's CPUs are affected by the "Meltdown" and "Spectre" flaws;
- 6           b. Whether the "Meltdown" and "Spectre" flaws put at risk confidential third-  
7 party information entrusted to Class members;
- 8           c. Whether efforts by Class members to monitor their computing resources and  
9 take other steps to mitigate the risks caused by the "Meltdown" and "Spectre" flaws are reasonable;
- 10           d. Whether Intel made any implied warranties or other representations in  
11 connection with the sale or marketing of its vulnerable CPUs;
- 12           e. Whether Intel breached any duties owed to Class members; and
- 13           f. Whether Intel violated Cal. Bus. & Prof. Code § 17200, et seq. or the New  
14 Mexico Unfair Trade Practices Act.

15           50. Plaintiff's claims arise out of the same common course of conduct giving rise to the  
16 claims of the other members of the Class. Plaintiff's interests are coincident with, and not  
17 antagonistic to, those of the other members of the Class.

18           51. Plaintiff is represented by counsel who are competent and experienced in the  
19 prosecution of class action litigation, including matters involving high-tech markets. Moreover,  
20 Plaintiff's counsel have retained renowned technical and industry experts who have significant  
21 experience with the matters at issue in this litigation.

22           52. The questions of law and fact common to the members of the Class predominate  
23 over any questions affecting only individual members, including legal and factual issues relating to  
24 liability and damages.

25           53. Class action treatment is a superior method for the fair and efficient adjudication of  
26 the controversy, in that, among other things, such treatment will permit a large number of similarly  
27 situated persons to prosecute their common claims in a single forum simultaneously, efficiently and  
28 without the unnecessary duplication of evidence, effort and expense that numerous individual

1 actions would engender. The benefits of proceeding through the class mechanism, including  
2 providing injured persons or entities with a method for obtaining redress for claims that might not  
3 be practicable to pursue individually, substantially outweigh any difficulties that may arise in  
4 management of this class action.

5 54. Absent a class action, most Class members would likely find the cost of litigating  
6 their claims prohibitively high and would therefore have no effective remedy at law. Because of  
7 the relatively small size of the individual Class members' claims compared to the anticipated costs  
8 of the litigation, it is likely that only a few Class members could afford to seek legal redress for the  
9 harms caused by Intel's design defects.

## 10 **CLAIMS FOR RELIEF**

### 11 **FIRST CLAIM FOR RELIEF**

#### 12 **Strict Liability**

13 55. Plaintiff, individually and on behalf of the Class, incorporates by reference all of the  
14 allegations contained in paragraphs 1 through 45 of this Complaint.

15 56. Plaintiff and Class members were harmed by the CPUs Intel manufactured and  
16 marketed, which were contained in, but also separate and apart from, the servers, PCs and other  
17 devices purchased.

18 57. Intel's CPUs contained manufacturing defects, or were defectively designed, for the  
19 reasons set forth above. As a result, Plaintiff and Class members now own servers, PCs and other  
20 devices with Intel CPUs that put at risk the confidential and protected third-party information and  
21 other sensitive data on their networks.

22 58. As a direct result of the manufacturing or design defect, Plaintiff and Class members  
23 have been harmed by having to incur mitigation and monitoring costs, in an amount to be  
24 determined at trial, and will continue to incur those expenses until their servers, PCs and other  
25 devices with defective Intel CPUs can be replaced with hardware that does not suffer from the  
26 defects.



1           66. Intel breached the implied warranty of merchantability because: (a) the defective  
2 Intel CPUs could not pass without objection in the trade because they are missing a key promoted  
3 characteristic, namely not exposing users to critical security vulnerabilities; (b) the CPUs were not  
4 of fair average quality; (c) were not adequately advertised, packaged, and/or labeled as omitting  
5 material facts as to the presence of the defects; or (d) they did not conform to the promises or  
6 affirmations of fact made by Defendant. Plaintiff and Class members did not receive goods as  
7 impliedly warranted by Intel to be “merchantable.” Moreover, as this was a latent defect that existed  
8 at time of purchase for the reasons described above, the CPUs are rendered unmerchantable.

9           67. Defendant also breached the implied warranty of fitness for a particular purpose as  
10 provided by law, including, inter alia, Cal. Comm. Code § 2316. Plaintiff and Class members  
11 purchased their servers, PCs and other computing devices with Intel CPUs for a particular purpose.  
12 Plaintiff and Class members could be reasonably expected to rely upon Intel’s skill and judgment  
13 in properly providing the CPUs without containing critical security vulnerabilities, and furnish  
14 goods suitable for their particular purpose, and thus would have no reason to believe otherwise.

15           68. Intel had reason to know that Plaintiff and Class members were relying on its skill  
16 and judgment to furnish suitable goods that would satisfy their particular purpose. Intel had reason  
17 to know of the particular purpose of these purchases, and that purchasers would be relying on their  
18 skill and judgment to ensure these computers would perform adequately and not subject them to  
19 critical security vulnerabilities.

20           69. The CPUs were not altered by Plaintiff or Class members.

21           70. The CPUs did not conform to these implied warranties when they left the exclusive  
22 control of Intel.

23           71. Plaintiff and Class members did not receive these goods as impliedly warranted.

24           72. All conditions precedent to seeking liability for breach of these implied warranties  
25 have been performed by or on behalf of Plaintiff and Class members. Intel has refused to recall,  
26 repair or replace, free of charge, all Intel CPUs or refund the prices paid for the CPUs.

27           73. As a direct and proximate cause of Intel’s breaches of implied warranties, Plaintiff  
28 and Class members have been injured and harmed, in an amount to be determined at trial.

**FOURTH CLAIM FOR RELIEF**

**Violation of Cal. Bus. & Prof. Code § 17200, et seq.:**  
**“Unfair” Business Practices**

74. Plaintiff, individually and on behalf of the Class, incorporates by reference all of the allegations contained in paragraphs 1 through 45 of this Complaint.

75. Plaintiff has standing to pursue this claim as AGH has suffered injury-in-fact and lost money or property as a result of the critical security vulnerabilities in Intel’s CPUs.

76. Intel’s business practices, including but not limited to its continued marketing of its defective CPUs after learning of the “Meltdown” and “Spectre” vulnerabilities, offend established public policy and/or are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to their customers. Additionally, Defendant’s conduct is “unfair” because Intel engaged in misleading and deceptive conduct, or to not sell defective products. Intel also concealed material facts from Plaintiff and Class members.

77. Intel’s business practices, including but not limited to its affirmative acts and material omissions are contrary to public and legislative policy and the harm it has, and continues to cause Plaintiff and members of the Class, far outweighs its utility.

78. As a result of Intel’s “unfair” business practices, Plaintiff and members of the Class spent money on servers, PCs and other computing devices that contain Intel’s defective CPUs.

79. Intel’s unfair business practices constitute a continuing course of unfair competition.

80. Plaintiff and Class members seek an order for injunctive relief to benefit the public, including a corrective advertising campaign, requiring Intel to make full disgorgement and restitution of all monies wrongfully obtained from Plaintiff and Class members, and all other relief permitted under Bus. & Prof. Code § 17200, et seq.

**FIFTH CLAIM FOR RELIEF**

**Violation of Cal. Bus. & Prof. Code § 17200, et seq.:**  
**“Deceptive” Business Practices**

81. Plaintiff, individually and on behalf of the Class, incorporates by reference all of the allegations contained in paragraphs 1 through 45 of this Complaint.

82. Plaintiff has standing to pursue this claim as AGH has suffered injury-in-fact and lost money or property as a result of the critical security vulnerabilities in Intel’s CPUs.

83. Intel’s business practices were “deceptive” because they were and are likely to deceive consumers, including Plaintiff and Class members, targeted by such omissions of material fact. Among other things, Intel failed to disclose material information to purchasers of servers, PCs and other computing devices containing Intel CPUs by concealing material facts relating to critical security vulnerabilities.

84. As a result of Intel’s “deceptive” conduct, Plaintiff and Class members spent money on servers, PCs and other computing devices with defective CPUs.

85. Intel’s deceptive business practices alleged herein constituted a continuing course of unfair competition.

86. Plaintiff and the Class seek an order for injunctive relief to benefit the public, including a corrective advertising campaign, requiring Intel to make full disgorgement and restitution of all monies that have been wrongfully obtained from Plaintiff and the Class, and all other relief permitted under Bus. & Prof. Code § 17200, et seq.

**SIXTH CLAIM FOR RELIEF**

**Violation of Cal. Bus. & Prof. Code § 17200, et seq.:**  
**“Unlawful” Business Practices**

87. Plaintiff, individually and on behalf of the Class, incorporate by reference all of the allegations contained in paragraphs 1 through 45 of this Complaint.

88. Plaintiff has standing to pursue this claim as AGH has suffered injury-in-fact and lost money or property as a result of the critical security vulnerabilities in Intel’s CPUs.



89. Intel's business practices, including but not limited to its continued marketing of its defective CPUs after learning of the "Meltdown" and "Spectre" vulnerabilities, constitute "unlawful" business practices because they violated California Civil Code § 1750, et seq., California Civil Code § 1790, et seq., 15 U.S.C. § 2301, et seq., among other laws, breached applicable warranties, and engaged in acts resulting in negligence and strict liability.

90. As a result of Intel's "deceptive" conduct, Plaintiff and Class members spent money on servers, PCs and other computing devices with defective CPUs.

91. Intel's deceptive business practices alleged herein constituted a continuing course of unfair competition.

92. Plaintiff and the Class seek an order for public injunctive relief to benefit the public, including a corrective advertising campaign, requiring Intel to make full disgorgement and restitution of all monies wrongfully obtained from Plaintiffs and the Class, and all other relief permitted under Bus. & Prof. Code § 17200, et seq.

## **SEVENTH CLAIM FOR RELIEF**

### **Violation of the New Mexico Unfair Trade Practices Act**

93. Plaintiff, individually and on behalf of the Class members operating in New Mexico, incorporate by reference all of the allegations contained in paragraphs 1 through 45 of this Complaint.

94. Defendant violated the New Mexico Unfair Trade Practices Act, N.M. Stat. Ann. § 57-12-1, et seq., which prohibits unfair or deceptive acts or practices.

95. Intel's business practices, including but not limited to its continued marketing of its defective CPUs after learning of the "Meltdown" and "Spectre" vulnerabilities, constitute unfair deceptive trade practices in that they are likely to deceive a reasonable consumer. A reasonable consumer expects or assumes that CPUs manufactured, marketed, and sold by Intel would not contain critical security vulnerabilities. Intel's misrepresentations and omissions concerning its defective CPUs are material and likely to deceive a reasonable consumer.

96. Among other things, and both before and after Google alerted Intel that it was aware of the CPU defects, Intel represented that its CPUs possessed certain characteristics and benefits

1 that they did not have and were fit for certain applications that they were not, Intel used  
2 exaggeration, innuendo, and ambiguity as to material facts regarding the fitness and quality of its  
3 CPUs in a manner that deceived or tended to deceive Plaintiff and New Mexico members of the  
4 Class and failed to state material facts regarding their CPUs that deceived or tended to deceive,  
5 which constitutes a deceptive trade practice within the meaning of the statute.

6 97. Intel also failed to deliver the quality of CPUs contracted for, in violation of the  
7 statute. Intel represented that its CPUs were fit to “prevent exposure to malicious code, viruses,  
8 cyber espionage, malware, and data theft,” and Defendant knew or should have known that Plaintiff  
9 and other Class members in New Mexico would purchase those CPUs through intermediaries in  
10 order to store or access sensitive third-party information.

11 98. As a result of Intel’s unfair and deceptive business practices, Plaintiff and Class  
12 members in New Mexico have been damaged in that they (a) purchased CPUs that they otherwise  
13 would not have purchased for the price they paid, (b) incurred substantial costs to monitor their  
14 networks and otherwise take steps to mitigate the risks to protected third-party information; and (c)  
15 will be required to replace servers, PCs and other devices with defective Intel CPUs when  
16 replacements are available that do not include the defect.

17 99. All of the wrongful conduct alleged herein occurred in the conduct of Intel’s  
18 business. Intel’s wrongful conduct is part of a pattern or generalized conduct that is still perpetuated  
19 and repeated, both in New Mexico and nationwide. Intel’s use of unfair and deceptive acts and  
20 practices was willful and knowing.

21 100. Plaintiff and Class members are entitled to damages in the amount of three times  
22 their actual damages or \$300 (whichever is greater). Plaintiff and Class members are also entitled  
23 to equitable relief, including restitution of all revenue accruing to Intel because of its unfair and  
24 deceptive practices; attorneys’ fees and costs; declaratory relief; and a permanent injunction  
25 enjoining Intel from its unfair and deceptive activity.

**PRAYER FOR RELIEF**

Plaintiff, individually and on behalf of all others similarly situated, requests the Court to enter judgment against Intel, as follows:

A. An order certifying the proposed Class, designating Plaintiff as the named representative of the Class, and designating the undersigned as Class Counsel;

B. An award of damages, including but not limited to compensatory, statutory and punitive damages, to Plaintiff and Class members in an amount to be determined at trial

C. An award of reasonable litigation expenses and attorneys' fees to Plaintiff and Class members;

D. An award of pre-judgment and post-judgment interest, as provided by law; and

E. An award of such other relief as may be appropriate under the circumstances.

**DEMAND FOR JURY TRIAL**

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any, and all issues in this action so triable of right.

Dated: February 23, 2018

/s/ Robert J. Gralewski, Jr.

Robert J. Gralewski, Jr.

**KIRBY McINERNEY LLP**

Robert J. Gralewski, Jr.

Fatima G. Brizuela

600 B Street, Suite 1900

San Diego, CA 92101

Telephone: (619) 398-4340

bgralewski@kmlp.com

fbrizuela@kmlp.com

**HINKLE SHANOR LLP**

Thomas M. Hnasko

Michael E. Jacobs

P.O. Box 2068

Santa Fe, NM 87504

Telephone: (505) 982-4554

thnasko@hinklelawfirm.com

mjacobs@hinklelawfirm.com

**HINKLE SHANOR LLP**

Andrew J. Cloutier

Lucas M. Williams

P.O. Box 10

Roswell, NM 88202

Telephone: (575) 622-6510

acloutier@hinklelawfirm.com

lwilliams@hinklelawfirm.com

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28